EUROPSKA
KOMISIJA

VISOKI PREDSTAVNIK
UNIJE ZA VANJSKE
POSLOVE I
SIGURNOSNU POLITIKU

Bruxelles, 6.4.2016.
JOIN(2016) 18 final

ZAJEDNIČKA KOMUNIKACIJA EUROPSKOM PARLAMENTU I VIJEĆU

Zajednički okvir za suzbijanje hibridnih prijetnji –

odgovor Europske unije

1. UVOD

Posljednjih se godina sigurnosno okruženje Europske unije drastično promijenilo. Ključnim se izazovima miru i stabilnosti u istočnom i južnom susjedstvu EU-a i dalje naglašava potreba za prilagodbom Unije i jačanju njezine uloge u jamčenju sigurnosti, sa snažnim naglaskom na uskoj povezanosti vanjske i unutarnje sigurnosti. Mnogi sadašnji izazovi miru, sigurnosti i blagostanju proizlaze iz nestabilnosti u neposrednom susjedstvu EU-a i promjenjivih oblika prijetnji. U svojim političkim smjernicama iz 2014. predsjednik Europske komisije Jean-Claude Juncker naglasio je potrebu za „stvaranjem jače Europe u području sigurnosti i obrane" i kombiniranjem europskih i nacionalnih instrumenata na učinkovitiji način nego dosad. Nadalje, nastavno na poziv Vijeća za vanjske poslove od 18. svibnja 2015., Visoka predstavnica je, blisko surađujući sa službama Komisije i Europskom obrambenom agencijom (EDA) i u dogovoru s državama članicama EU-a, poduzela mjere te predstavila ovaj zajednički okvir s provedivim prijedlozima radi suzbijanja hibridnih prijetnji i jačanja otpornosti EU-a i država članica, kao i partnera.[1] U lipnju 2015. Europsko vijeće ponovno je naglasilo potrebu za mobiliziranjem instrumenata EU-a kako bi se pomoglo u suzbijanju hibridnih prijetnji.[2]

Iako se definicije hibridnih prijetnji razlikuju te moraju biti fleksibilne kako bi se odgovorilo na njihovu promjenjivu prirodu, konceptom se nastoji obuhvatiti kombinacija prisilne i subverzivne aktivnosti te konvencionalnih i nekonvencionalnih metoda (tj. diplomatskih, vojnih, gospodarskih i tehnoloških) koje državni ili nedržavni dionici mogu upotrebljavati na koordiniran način kako bi postigli specifične ciljeve, pritom službeno ne objavljujući rat. Naglasak je obično na iskorištavanju slabosti cilja i stvaranju nejasnoća kako bi se omeli procesi odlučivanja. Velike kampanje dezinformiranja javnosti, u kojima se koriste društvene mreže za kontrolu političkog prikaza ili radikalizaciju, novačenje i usmjeravanje zamjenskih dionika, mogu biti pokretači hibridnih prijetnji.

Budući da je suzbijanje hibridnih prijetnji povezano s nacionalnom sigurnošću i obranom te održavanjem zakona i reda, države članice imaju primarnu odgovornost jer je većina nacionalnih slabosti specifična za pojedine države. Međutim, mnoge se države članice EU-a suočavaju sa zajedničkim prijetnjama koje mogu biti usmjerene i na prekogranične mreže ili infrastrukture. Takve se prijetnje mogu učinkovitije ukloniti koordiniranim odgovorom na razini EU-a koristeći se politikama i instrumentima EU-a kako bi se unaprijedila europska solidarnost i uzajamna pomoć te iskoristio pun potencijal Ugovora iz Lisabona. Politike i instrumenti EU-a mogu imati ključnu ulogu u davanju dodatne vrijednosti podizanju svijesti, a njima se uvelike to već i čini. Time se državama članicama pomaže da budu otpornije na zajedničke prijetnje. Vanjsko djelovanje Unije koje je predloženo unutar ovog okvira vođeno je načelima utvrđenima u članku 21. Ugovora o Europskoj uniji (UEU), koja uključuju demokraciju, vladavinu prava,

[1] Zaključci Vijeća o zajedničkoj obrambenoj i sigurnosnoj politici (ZSOP), svibanj 2015. (Consilium 8971/15).
[2] Zaključci Europskog vijeća, lipanj 2015. (EUCO 22/15).

univerzalnost i nedjeljivost ljudskih prava te poštovanje načela Povelje Ujedinjenih naroda i međunarodnog prava.[3]

Ovom se Zajedničkom komunikacijom nastoji promicati holistički pristup kojim će se EU-u, u suradnji s državama članicama, omogućiti da suzbije hibridne prijetnje stvarajući sinergiju među svim relevantnim instrumentima i potičući blisku suradnju među svim relevantnim dionicima.[4] Te se aktivnosti nastavljaju na postojeće strategije i sektorske politike kojima se doprinosi postizanju veće sigurnosti. Posebice, alati kojima se isto tako može doprinijeti suzbijanju hibridnih prijetnji su Europski program sigurnosti,[5] globalna strategija EU-a za vanjsku i sigurnosnu politiku te europski akcijski plan u području obrane koji predstoje,[6] Strategija EU-a za kibernetičku sigurnost,[7] Strategija energetske sigurnosti[8] i Strategija Europske unije za sigurnosnu zaštitu u pomorstvu.[9]

Budući da i NATO radi na suzbijanju hibridnih prijetnji te da je Vijeće za vanjske poslove predložilo pojačanu suradnju i koordinaciju u ovom području, nekim se prijedlozima nastoji poboljšati suradnja EU-a i NATO-a u suzbijanju hibridnih prijetnji.

U predloženom je odgovoru naglasak na sljedećim elementima: podizanju svijesti, jačanju otpornosti, sprečavanju krize, odgovoru na krizu i oporavku.

2. PREPOZNAVANJE HIBRIDNE PRIRODE PRIJETNJE

Hibridnim se prijetnjama nastoje iskoristiti slabosti pojedine države i često ugroziti temeljna demokratska prava i slobode. Prvi bi korak bila suradnja Visoke predstavnice i Komisije s državama članicama radi stjecanja boljeg uvida u stanje s pomoću praćenja i provjere rizika potencijalno usmjerenih na slabosti EU-a. Komisija razvija metodologije ocjene sigurnosnog rizika kako bi se mogli informirati donositelji odluka te radi promicanja oblikovanja politike temeljene na procjeni rizika u raznim područjima, od sigurnosti zračnog prometa do financiranja terorizma i pranja novca. Osim toga, bilo bi važno da države članice provedu istraživanje o utvrđivanju područja koja su podložna hibridnim prijetnjama. Cilj bi bio utvrditi pokazatelje hibridnih prijetnji, uklopiti ih u mehanizme ranog upozoravanja i postojećih procjena rizika te ih razmjenjivati prema potrebi.

<u>Mjera 1.</u>: države članice, koje prema potrebi podupiru Komisija i Visoka predstavnica, pozivaju se da provedu istraživanje o hibridnom riziku radi utvrđivanja ključnih

[3] Povelja EU-a o temeljnim pravima obvezujuća je za institucije i države članice pri provedbi prava Unije.
[4] Mogući zakonodavni prijedlozi bit će podložni zahtjevima Komisije za bolju regulativu, u skladu sa smjernicama Komisije za bolju regulativu, SWD(2015) 111.
[5] COM(2015) 185 final
[6] Bit će predstavljeni 2016.
[7] Okvir politike kibernetičke obrane EU-a (Consilium 15585/14) i Zajednička komunikacija o Strategiji Europske unije za kibernetičku sigurnost: otvoren, siguran i zaštićen kibernetički prostor, veljača 2013. (JOIN(2013)1)
[8] Zajednička komunikacija o Europskoj strategiji energetske sigurnosti, veljača 2014. **(**SWD(2014) 330)
[9] Zajednička komunikacija – Za otvoreno i sigurno globalno pomorsko dobro: elementi za strategiju sigurnosne zaštite u pomorstvu Europske unije, JOIN(2014) 9 final – 6.3.2014.

slabosti, uključujući specifične pokazatelje hibridnih prijetnji, koje potencijalno utječu na nacionalne i paneuropske strukture i mreže.

3. ORGANIZIRANJE ODGOVORA EU-A: PODIZANJE SVIJESTI

3.1. Jedinica EU-a za otkrivanje hibridnih prijetnji (*EU Hybrid Fusion Cell*)

Nužno je da EU, u suradnji s državama članicama, ima dovoljan uvid u stanje radi utvrđivanja svake promjene u sigurnosnom okruženju povezane s hibridnom aktivnošću koju su uzrokovali državni ili nedržavni dionici. Za učinkovito suzbijanje hibridnih prijetnji važno je poboljšati razmjenu informacija i promicati relevantnu razmjenu obavještajnih podataka među sektorima te između Europske unije, njezinih država članica i partnera.

Jedinica EU-a za otkrivanje hibridnih prijetnji bit će jedinstvena točka za analizu hibridnih prijetnji, uspostavljena u okviru Centra EU-a za analizu obavještajnih podataka (EU INTCEN) Europske službe za vanjsko djelovanje (ESVD). Jedinica za otkrivanje hibridnih prijetnji primala bi, analizirala i razmjenjivala povjerljive i dostupne informacije koje se posebno odnose na pokazatelje i upozorenja o hibridnim prijetnjama, a koje pružaju razni dionici unutar ESVD-a (uključujući delegacije EU-a), Komisija (uključujući agencije EU-a[10]) i države članice. U suradnji sa sličnim postojećim tijelima na razini EU-a i nacionalnoj razini[11], jedinica za otkrivanje hibridnih prijetnji analizirala bi vanjske aspekte hibridnih prijetnji koji utječu na EU i susjedstvo kako bi se brzo analizirali relevantni incidenti i olakšali procesi donošenja strateških odluka EU-a, uključujući pridonošenje procjenama sigurnosnog rizika koje se provode na razini EU-a. S analitičkim rezultatima jedinice za otkrivanje hibridnih prijetnji postupalo bi se u skladu s pravilima Europske unije o povjerljivim informacijama i zaštiti podataka.[12] Jedinica bi trebala surađivati s postojećim tijelima na razini EU-a i nacionalnoj razini. Države članice trebale bi uspostaviti nacionalne kontaktne točke povezane s jedinicom EU-a za otkrivanje hibridnih prijetnji. Osoblje unutar i izvan EU-a (uključujući one angažirane u delegacijama, operacijama i misijama EU-a) te u državama članicama isto bi tako trebalo biti osposobljeno za prepoznavanje prvih znakova hibridnih prijetnji.

<u>Mjera 2.</u>: osnivanje jedinice EU-a za otkrivanje hibridnih prijetnji unutar postojeće strukture EU INTCEN-a, koja može primati i analizirati povjerljive i dostupne informacije o hibridnim prijetnjama. Države članice pozivaju se da uspostave nacionalne kontaktne točke za prijavu hibridnih prijetnji kako bi se osigurala suradnja i sigurna komunikacija s jedinicom EU-a za otkrivanje hibridnih prijetnji.

[10] Sukladno svojim mandatima.
[11] Primjerice, Europolovi Europski centar za borbu protiv kibernetičkog kriminala i Europski centar za borbu protiv terorizma, Frontex i Tim za hitne računalne intervencije EU-a (CERT-EU).
[12] Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995.

3.2. Strateška komunikacija

Počinitelji hibridnih prijetnji mogu sustavno širiti dezinformacije i ciljanim kampanjama na društvenim mrežama te na taj način nastojati radikalizirati pojedince, destabilizirati društvo i kontrolirati politički prikaz. Ključna je sposobnost odgovora na hibridne prijetnje primjenom dobro osmišljene strategije **strateške komunikacije**. Osiguravanje brzih činjeničnih odgovora i podizanje javne svijesti o hibridnim prijetnjama najvažniji su čimbenici stvaranja socijalne otpornosti.

U strateškoj bi se komunikaciji trebali u potpunosti koristiti alati društvenih medija, kao i tradicionalni vizualni, audio i internetski mediji. EEAS bi, na temelju aktivnosti radnih skupina East StratCom i Arab StratCom, trebao optimizirati korištenje lingvistima koji tečno govore relevantne jezike koji nisu službeni jezici EU-a te stručnjake za društvene medije s mogućnošću nadziranja informacija pristiglih iz trećih zemalja i osigurati ciljanu komunikaciju kao odgovor na dezinformacije. Nadalje, države članice trebale bi razviti koordinirane mehanizme strateške komunikacije radi poticanja pripisivanja informacija i suprotstavljanja dezinformacijama kako bi se otkrile hibridne prijetnje.

<u>Mjera 3.</u>: Visoka predstavnica će s državama članicama istražiti načine ažuriranja i koordinacije kapaciteta radi omogućivanja proaktivne strateške komunikacije i optimiranja praćenja medija i korištenja lingvističkim stručnjacima.

3.3. Centar izvrsnosti za suzbijanje hibridnih prijetnji

Koristeći se iskustvom pojedinih država članica i partnerskih organizacija[13], jedan multinacionalni institut ili mreža multinacionalnih instituta mogli bi djelovati kao centri izvrsnosti koji se bave pitanjem hibridnih prijetnji. U takvom bi se centru mogli usredotočiti na načine provedbe hibridnih strategija te potaknuti razvoj novih koncepata i tehnologija u privatnom sektoru i industriji radi pružanja podrške državama članicama u jačanju otpornosti. Tim bi se istraživanja moglo doprinijeti usklađivanju nacionalnih politika, doktrina i koncepata s politikama, doktrinama i konceptima EU-a, kao i osiguravanju da se pri donošenju odluka uzimaju u obzir složenosti i nejasnoće povezane s hibridnim prijetnjama. U takvom bi se centru mogli oblikovati programi za napredna istraživanja i vježbe kako bi se pronašla praktična rješenja za postojeće izazove koje donose hibridne prijetnje. Snaga takvog centra bila bi u stručnosti njegovih multinacionalnih i međusektorskih sudionika iz civilnog i vojnog te privatnog i akademskog sektora.

Takav bi centar blisko surađivao s postojećim[14] centrima izvrsnosti EU-a i NATO-a[15] kako bi se iskoristili uvidi u hibridne prijetnje dobiveni na temelju kibernetičke obrane, strateške komunikacije, civilno-vojne suradnje, energetike i odgovora na krizu.

[13] Centri izvrsnosti NATO-a.
[14] Npr. Institut EU-a za sigurnosne studije (EU ISS), tematski centri izvrsnosti EU-a u vezi s pitanjima KBRN-a.
[15] http://www.nato.int/cps/en/natohq/topics_68372.htm

<u>Mjera 4.</u>: države članice pozvane su razmotriti uspostavu centra za izvrsnost za suzbijanje hibridnih prijetnji.

4. ORGANIZIRANJE ODGOVORA EU-A: JAČANJE OTPORNOSTI

Otpornost je sposobnost podnošenja stresa te sposobnost oporavka nakon izazova. Kako bi se učinkovito suzbile hibridne prijetnje, potrebno je ukloniti potencijalne slabosti ključnih infrastruktura, lanaca opskrbe i društva. Oslanjajući se na instrumente i politike EU-a infrastruktura na razini EU-a mogla bi postati otpornija.

4.1. Zaštita kritične infrastrukture

Važno je zaštititi kritičnu infrastrukturu (npr. lanac opskrbe energijom, promet) jer bi nekonvencionalan napad na bilo koju „meku metu" koji bi izvršili počinitelji hibridnih prijetnji mogao dovesti do ozbiljnih gospodarskih ili društvenih problema. Kako bi se zaštitila kritična infrastruktura, Europskim programom zaštite kritične infrastrukture[16] (EPCIP) omogućava se međusektorski sustavni pristup utemeljen na svestranom razmatranju rizika, uzimajući u obzir međuovisnosti na temelju provedbe mjera u okviru područja djelovanja koja se odnose na sprečavanje, pripravnost i odgovor. Direktivom o europskoj kritičnoj infrastrukturi[17] utvrđuje se postupak za utvrđivanje i označivanje europske kritične infrastrukture (EKI) i zajednički pristup procjeni potrebe za unapređenjem njezine zaštite. Posebno je potrebno ponovno pokrenuti nastojanja u okviru Direktive kako bi se poboljšala otpornost ključne infrastrukture u vezi s prometom (npr. glavni aerodromi i trgovačke luke EU-a). Komisija će procijeniti je li potrebno razvijati zajedničke alate, uključujući pokazatelje, kako bi se poboljšala otpornost kritičke infrastrukture na hibridne prijetnje u svim relevantnim sektorima.

<u>Mjera 5.</u>: Komisija će, u suradnji s državama članicama i zainteresiranim stranama, utvrditi zajedničke alate, uključujući pokazatelje, s ciljem poboljšanja zaštite i otpornosti kritične infrastrukture na hibridne prijetnje u relevantnim sektorima.

4.1.1. Energetske mreže

Nesmetana proizvodnja i distribucija energije iznimno su važne za EU te bi mu znatni prekidi opskrbe električnom energijom mogli naštetiti. Ključni element u suzbijanju hibridnih prijetnji daljnja je diversifikacija izvora energije EU-a, opskrbljivača i opskrbnih pravaca kako bi se mogla zajamčiti sigurnija i otpornija opskrba energijom. Komisija isto tako provodi procjene rizika i sigurnosti („testove otpornosti") elektrana EU-a. Nastojanja se u okviru Strategije energetske unije pojačavaju kako bi se osigurala diversifikacija energije: primjerice, južni plinski koridor omogućuje da plin iz Kaspijske regije dođe do Europe, a u sjevernoj Europi omogućuje uspostavljanje čvorišta ukapljenog plina s više opskrbljivača. Ovaj primjer treba slijediti u središnjoj i istočnoj

[16] Komunikacija Komisije o Europskom programu zaštite kritične infrastrukture, 12.12.2006., COM(2006) 786 final

[17] Direktiva Vijeća 2008/114/EZ od 8. prosinca 2008. o utvrđivanju i označivanju europske kritične infrastrukture i procjeni potrebe poboljšanja njezine zaštite, SL L 345 od 23.12.2008.

Europi i na Sredozemlju gdje su u tijeku radovi na plinskom čvorištu.[18] Razvoj tržišta za ukapljeni prirodni plin isto će tako pozitivno doprinijeti tom cilju.

Komisija podupire razvoj i donošenje najviših standarda sigurnosti kad je riječ o nuklearnim materijalima i postrojenjima te na taj način pojačava otpornost. Komisija potiče dosljedni prijenos i provedbu Direktive o nuklearnoj sigurnosti[19] kojom se utvrđuju pravila za sprečavanje nesreća i ublažavanje posljedica nesreća te provedbu odredaba Direktive o osnovnim sigurnosnim normama[20] kad je riječ o međunarodnoj suradnji u pogledu pripravnosti i odgovora u hitnim slučajevima, posebno među državama članicama i susjednim državama.

Mjera 6.: Komisija će, u suradnji s državama članicama, podupirati nastojanja za diversifikacijom izvora energije i promicati standarde sigurnosti kako bi se pojačala otpornost nuklearne infrastrukture.

4.1.2. Sigurnost prometa i opskrbnog lanca

Promet je ključan za funkcioniranje Unije. Hibridni napadi na prometnu infrastrukturu (poput onih na zračne luke, cestovnu infrastrukturu, luke i željeznice) mogu imati ozbiljne posljedice te dovesti do prekida u odvijanju prometa i do ometanja opskrbnih lanaca. Komisija u okviru provedbe zakonodavstva za sigurnosnu zaštitu zračnog prometa i sigurnosnu zaštitu u pomorstvu[21] provodi redovite inspekcije[22] i kroz svoj rad u području sigurnosti kopnenog prometa nastoji otkloniti nove hibridne prijetnje. U tom se kontekstu raspravlja o okviru EU-a na temelju revidirane Uredbe o sigurnosti zračnog prometa[23], kao dijela Strategije zrakoplovstva za Europu.[24] Nadalje, prijetnje sigurnosnoj zaštiti u pomorstvu nastoje se otkloniti u okviru Strategije Europske unije za sigurnosnu

[18] Dosadašnji napredak možete vidjeti u Stanju energetske unije 2015. COM (2015) 572 final

[19] Direktiva Vijeća 2009/71/Euratom od 25. lipnja 2009. o uspostavi okvira Zajednice za nuklearnu sigurnost nuklearnih postrojenja, kako je izmijenjena Direktivom Vijeća 2014/87/Euratom od 8. srpnja 2014.

[20] Direktiva Vijeća 2013/59/Euratom od 5. prosinca 2013. o osnovnim sigurnosnim standardima za zaštitu od opasnosti koje potječu od izloženosti ionizirajućem zračenju, i o stavljanju izvan snage direktiva 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom i 2003/122/Euratom

[21] Uredba (EZ) br. 300/2008 Europskog parlamenta i Vijeća od 11. ožujka 2008. o zajedničkim pravilima u području zaštite civilnog zračnog prometa i stavljanju izvan snage Uredbe (EZ) br. 2320/2002; Provedbena uredba Komisije (EU).. 2015/1998 od 5. studenoga 2015. o utvrđivanju detaljnih mjera za provedbu zajedničkih osnovnih standarda iz područja zaštite zračnog prometa; Direktiva 2005/65/EZ Europskog parlamenta i Vijeća od 26. listopada 2005. o jačanju sigurnosne zaštite luka; Uredba (EZ) br. 725/2004 Europskog parlamenta i Vijeća od 31. ožujka 2004. o jačanju sigurnosne zaštite brodova i luka.

[22] U skladu s pravom EU-a Komisija mora provoditi inspekcije kako bi osigurala da države članice ispravno provode zahtjeve za sigurnosnu zaštitu zračnog prometa i sigurnosnu zaštitu u pomorstvu. To uključuje inspekciju odgovarajućih nadležnih tijela u državama članicama, kao i zračnih luka, luka, zračnih prijevoznika, brodova te subjekata koji provode mjere sigurnosti. Inspekcijama Komisije nastoji se osigurati da države članice u potpunosti provode standarde EU-a.

[23] Uredba Komisije (EU) 2016/4 od 5. siječnja 2016. o izmjeni Uredbe (EZ) br. 216/2008 Europskog parlamenta i Vijeća u pogledu bitnih zahtjeva u pogledu zaštite okoliša; Uredba (EZ) br. 216/2008 od 20.2.2008. o zajedničkim pravilima u području civilnog zrakoplovstva i osnivanju Europske agencije za sigurnost zračnog prometa.

[24] Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija: Strategija zrakoplovstva za Europu, COM/2015/0598 final, 7.12.2015.

zaštitu u pomorstvu i njezina Akcijskog plana.[25] Akcijskim planom omogućava se EU-u i državama članicama da se sveobuhvatno suoče s izazovima sigurnosne zaštite u pomorstvu, uključujući suzbijanje hibridnih prijetnji, kroz međusektorsku suradnju civilnih i vojnih dionika radi zaštite kritične pomorske infrastrukture, svjetskog lanca opskrbe, pomorske trgovine te pomorskih prirodnih i energetskih resursa. O sigurnosti međunarodnog lanca opskrbe raspravlja se i u Strategiji za upravljanje rizicima u carinskim pitanjima te Akcijskom planu.[26]

Mjera 7.: Komisija će pratiti nove prijetnje diljem prometnog sektora i prema potrebi ažurirati zakonodavstvo. U provedbi Strategije EU-a za sigurnosnu zaštitu u pomorstvu te Strategije za upravljanje rizicima u carinskim pitanjima i Akcijskog plana, Komisija i Visoka predstavnica će (u okviru svojih nadležnosti) u suradnji s državama članicama ispitati način postupanja u slučaju hibridne prijetnje, posebno one koja se odnosi na ključnu prometnu infrastrukturu.

4.1.3. Svemir

Cilj hibridnih prijetnji mogle bi biti svemirske infrastrukture, a to bi uzrokovalo višesektorske posljedice. EU je izradio okvir potpore za nadzor i praćenje u svemiru[27] radi umrežavanja sredstava u vlasništvu država članica kako bi[28] identificiranim korisnicima (državama članicama, institucijama EU-a, vlasnicima i operaterima svemirskih letjelica i tijelima za civilnu zaštitu) pružile usluge nadzora i praćenja u svemiru. U kontekstu predstojeće svemirske strategije za Europu Komisija će istražiti njezin daljnji razvoj kako bi pratila hibridne prijetnje svemirskim infrastrukturama.

Satelitske komunikacije (SatCom) ključne su za upravljanje krizom, djelovanje u slučaju katastrofa, policiju, granični i obalni nadzor. One su okosnica velikih infrastruktura kao što su prijevoz, svemir ili zrakoplovni sustavi na daljinsko upravljanje. U skladu s pozivom Europskog vijeća za pripremu sljedeće generacije satelitskih komunikacija vlade (GovSatCom), Komisija u suradnji s Europskom obrambenom agencijom procjenjuje načine objedinjavanja potražnje u kontekstu svemirske strategije i europskog akcijskog plana u području obrane koji predstoje.

Brojne kritične infrastrukture oslanjaju se na precizno vrijeme razmjene informacija kako bi uskladile svoje mreže (npr. energetske ili telekomunikacijske) ili vremenski označile transakcije (npr. financijska tržišta). Ovisnošću o jedinstvenom vremenskom sinkronizacijskom signalu u okviru globalnog sustava za satelitsku navigaciju ne omogućava se otpornost koja je potrebna kako bi se suzbile hibridne prijetnje. Program

[25] U prosincu 2014. Vijeće je donijelo Akcijski plan za provedbu Strategije Europske unije za sigurnosnu zaštitu u pomorstvu; http://ec.europa.eu/maritimeaffairs/policy/maritime-security/doc/20141216-action-plan_en.pdf

[26] Komunikacija Komisije Europskom parlamentu, Vijeću i Europskom gospodarskom i socijalnom odboru o Strategiji EU-a i Akcijskom planu za upravljanjem rizicima u carinskim pitanjima: Rješavanje rizika, jačanje sigurnosti lanca opskrbe i olakšavanje trgovine, COM (2014) 527 final

[27] Vidjeti Odluku 541/2014/ Europskog parlamenta i Vijeća.

[28] Poput upozorenja o izbjegavanju sudara u orbiti, upozorenja o prekidima i sudarima te rizičnom povratu svemirskih objekata u Zemljinu atmosferu.

Galileo, europski satelitski navigacijski sustav, mogao bi biti drugi pouzdan vremenski izvor.

<u>Mjera 8.</u>: u kontekstu svemirske strategije i europskog akcijskog plana u području obrane koji predstoje, Komisija će predložiti povećanje otpornosti svemirske infrastrukture na hibridne prijetnje, posebno kroz mogućnost proširivanja nadzora i praćenja u svemiru kako bi se obuhvatile hibridne prijetnje, pripreme za sljedeću generaciju GovSatCom-a na europskoj razini te uvođenje programa Galileo u područje ključnih infrastruktura koje su ovisne o sinkronizaciji vremena.

4.2. Obrambeni kapaciteti

Potrebno je ojačati obrambene kapacitete kako bi se povećala otpornost EU-a na hibridne prijetnje. Važno je utvrditi relevantna ključna područja kapaciteta, npr. nadzorne i izviđačke kapacitete. Europska obrambena agencija može biti katalizator razvoja vojnih kapaciteta povezanih s hibridnim prijetnjama (npr. skraćivanje ciklusa razvoja obrambenih kapaciteta, ulaganje u tehnologiju, sustave i prototipove i otvaranje poslovanja obrane inovativnim komercijalnim tehnologijama). Moguće mjere mogu se istražiti u okviru predstojećeg europskog akcijskog plana u području obrane.

<u>Mjera 9.</u>: Visoka predstavnica, koju prema potrebi podupiru države članice, u suradnji s Komisijom predložit će projekte o prilagođavanju obrambenih kapaciteta i razvoju od važnosti za EU, posebno kako bi se suzbile hibridne prijetnje jednoj državi članici ili više njih.

4.3. Zaštita javnog zdravlja i sigurnost hrane

Zdravlje stanovništva moglo bi biti ugroženo manipulacijom zaraznih bolesti ili kontaminacijom hrane, tla, zraka i pitke vode kemijskim, biološkim, radiološkim ili nuklearnim (KBRN) tvarima. Osim toga, namjernim širenjem bolesti životinja ili biljaka mogla bi se ozbiljno ugroziti sigurnost hrane u Uniji uzrokujući znatne gospodarske i društvene učinke na ključna područja prehrambenog lanca u EU-u. Koristeći se tim metodama, postojeće se strukture EU-a za zdravstvenu sigurnost, zaštitu okoliša i sigurnost hrane mogu upotrijebiti kao odgovor na hibridne prijetnje.

Prema zakonodavstvu EU-a o prekograničnim prijetnjama zdravlju[29], postojećim se mehanizmima koordinira pripravnost za ozbiljne prekogranične prijetnje zdravlju povezujući države članice, agencije EU-a i znanstvene odbore[30] preko sustava ranog upozorenja i odgovora. Odbor za zdravstvenu sigurnost koji koordinira odgovore država

[29] Odluka br. 1082/2013/EU Europskog parlamenta i Vijeća od 22. listopada 2013. o ozbiljnim prekograničnim prijetnjama zdravlju i o stavljanju izvan snage Odluke br. 2119/98/EZ, SL L 293/1, 5.11.2013.

[30] Odluka Komisije C(2015) 5383 od 7.8.2015. o osnivanju znanstvenih odbora u području javnog zdravlja, sigurnosti potrošača i okoliša.

članica na prijetnje može djelovati kao središnja točka za slabosti u javnom zdravlju[31] koja će u smjernicama o obavještavanju o kriznoj situaciji te postupcima izgradnje kapaciteta (simulacija krize) s državama članicama obuhvatiti hibridne prijetnje. U području sigurnosti hrane nadležna tijela razmjenjuju informacije o analizama rizika preko Sustava brzog uzbunjivanja za hranu i hranu za životinje (RASFF) i zajedničkog sustava za upravljanje rizikom (CRMS) za carinu kako bi se nadzirali zdravstveni rizici koje predstavlja kontaminirana hrana. Kad je riječ o zdravlju životinja i biljaka, revizijom pravnog okvira EU-a[32] dodat će se novi elementi postojećim „alatima"[33] radi bolje pripremljenosti i na hibridne prijetnje.

Mjera 10.: Komisija će u suradnji s državama članicama podići razinu svijesti i otpora na hibridne prijetnje unutar postojećih mehanizama pripravnosti i koordinacije, posebno Odbora za zdravstvenu sigurnost.

4.4. Kibernetička sigurnost

EU ima veliku korist od svojeg međusobno povezanog i digitaliziranog društva. Kibernetički bi napadi mogli ugroziti digitalne usluge diljem EU-a i počinitelji hibridnih prijetnji mogli bi koristiti takve napade. Jačanje otpornosti komunikacijskih i informacijskih sustava u Europi važno je kako bi se poduprlo jedinstveno digitalno tržište. Strategijom EU-a za kibernetičku sigurnost i Europskim programom sigurnosti pruža se opći strateški okvir za inicijative EU-a u područjima kibernetičke sigurnosti i kibernetičkog kriminala. EU je aktivan u podizanju svijesti, razvoju mehanizama suradnje i odgovora u okviru rezultata Strategije za kibernetičku sigurnost. Posebno se predložena Direktiva o mrežnoj i informacijskoj sigurnosti (NIS)[34] bavi rizicima kibernetičke sigurnosti kad je riječ o širokom rasponu ključnih pružatelja usluga u području energetike, prijevoza, financija i zdravlja. Ti bi pružatelji, kao i pružatelji ključnih digitalnih usluga (npr. računalstva u oblaku) trebali poduzeti odgovarajuće mjere sigurnosti i prijaviti ozbiljne incidente nacionalnim nadležnim tijelima ako primijete bilo kakve hibridne značajke. Kad zakonodavci donesu Direktivu, njezinim bi se učinkovitim prijenosom i provedbom ojačali kapaciteti kibernetičke sigurnosti diljem država članica jačanjem njihove suradnje u području kibernetičke sigurnosti razmjenom informacija i najboljih praksi u suzbijanju hibridnih prijetnji. Direktivom se posebno predviđa uspostavljanje mreže 28 nacionalnih timova za rješavanje računalnih sigurnosnih

[31] U skladu s Odlukom br. 1082/2013/EU Europskog parlamenta i Vijeća od 22. listopada 2013. o ozbiljnim prekograničnim prijetnjama zdravlju i o stavljanju izvan snage Odluke br. 2119/98/EZ, SL L 293/1.

[32] Uredba 2016/429 Europskog parlamenta i Vijeća o prenosivim bolestima životinja te o izmjeni i stavljanju izvan snage određenih akata u području zdravlja životinja („Zakon o zdravlju životinja"), SL L 84), 31.3.2016. U pogledu Uredbe Europskog parlamenta i Vijeća o zaštitnim mjerama protiv organizama štetnih za bilje („Zakon o zdravlju bilja"), Europski parlament i Vijeće postigli su 16. prosinca 2015. politički dogovor o tekstu.

[33] Npr. banke cjepiva EU-a, sofisticiran elektronički informacijski sustav za bolesti životinja, veće obveze za mjere laboratorija i drugih subjekata koji se bave patogenima.

[34] Prijedlog Komisije za direktivu Europskog parlamenta i Vijeća o mjerama za osiguravanje visoke zajedničke razine mrežne i informacijske sigurnosti u Uniji COM(2013) 48 final – 7/2/2013. O predloženoj je Direktivi postignut politički dogovor Vijeća EU-a i Europskog parlamenta i ona bi trebala ubrzo biti službeno donesena.

incidenata (CSIRT) te CERT-EU-a[35] kako bi se operativna suradnja nastavila na dobrovoljnoj osnovi.

Kako bi potaknula javno-privatnu suradnju i pristup kibernetičkoj sigurnosti diljem EU-a, Komisija je uspostavila platformu NIS s pomoću koje pruža smjernice o najboljoj praksi za upravljanje rizikom. Države članice određuju sigurnosne zahtjeve i načine obavještavanja o nacionalnim incidentima, a Komisija potiče visok stupanj konvergencije pristupa upravljanja rizikom, posebno se oslanjajući na Agenciju Europske unije za mrežnu i informacijsku sigurnost (ENISA).

***Mjera 11.**: Komisija prije svega potiče države članice da ustanove i u potpunosti iskoriste mrežu među 28 CSIRT-ova i CERT-EU-ova, kao i okvir za stratešku suradnju. Komisija bi u suradnji s državama članicama trebala osigurati da su sektorske inicijative koje su usmjerene na kibernetičke prijetnje (npr. zračni promet, energetika, pomorstvo) u skladu s međusektorskim kapacitetima koje obuhvaća Direktiva o mrežnoj i informacijskoj sigurnosti radi prikupljanja podataka, stručnog znanja i brzih odgovora.*

4.4.1. Industrija

Većim oslanjanjem na računalstvo u oblaku i masovne podatke povećala se osjetljivost na hibridne prijetnje. Strategijom jedinstvenog digitalnog tržišta pruža se ugovorno javno-privatno partnerstvo o kibernetičkoj sigurnosti[36] koje će se usredotočiti na istraživanje i inovaciju te pomoći Uniji da zadrži visoku razinu tehnoloških kapaciteta u tom području. Ugovornim javno-privatnim partnerstvima stvorit će se povjerenje među različitim dionicima na tržištu te će razvijati sinergije ponude i potražnje. Ugovorno javno-privatno partnerstvo i prateće mjere prvenstveno će se usredotočiti na proizvode i usluge civilne kibernetičke sigurnosti, a zbog rezultata tih inicijativa korisnici tehnologije trebali bi biti bolje zaštićeni od hibridnih prijetnji.

***Mjera 12.**: Komisija će, zajedno s državama članicama, surađivati s industrijom u kontekstu ugovornog javno-privatnog partnerstva o kibernetičkoj sigurnosti kako bi se razvile i ispitale tehnologije radi bolje zaštite korisnika i infrastruktura protiv kibernetičkih aspekata hibridnih prijetnji.*

4.4.2. Energetika

Pojava pametnih domova i uređaja te razvoj pametne mreže čime se povećava digitalizacija energetskog sustava isto tako dovodi do povećane osjetljivosti na kibernetičke napade. Europskom strategijom energetske sigurnosti[37] i Strategijom energetske unije[38] podržava se pristup utemeljen na svestranom razmatranju rizika u koji

[35] Tim institucija EU-a za hitne računalne intervencije (CERT-EU).
[36] Bit će pokrenuto sredinom 2016.
[37] Komunikacija Komisije Europskom parlamentu i Vijeću: Europska strategija energetske sigurnosti – COM/2014/0330, final
[38] Komunikacija o okvirnoj strategiji za otpornu energetsku uniju s naprednom klimatskom politikom – COM/2015/080, final

je uključena otpornost na hibridne prijetnje. Tematska mreža o zaštiti ključne energetske infrastrukture potiče suradnju među operaterima u energetskom sektoru (nafta, plin, struja). Komisija je pokrenula mrežnu platformu za analizu i razmjenu informacija o prijetnjama i incidentima.[39] Isto tako sa zainteresiranim stranama razvija[40] sveobuhvatnu strategiju energetskog sektora za kibernetičku sigurnost u pametnim mrežama kako bi se smanjile slabosti. Iako su tržišta električne energije sve više integrirana, pravila i postupci za rješavanje kriznih situacija i dalje su nacionalni. Trebamo osigurati suradnju vlada u pripravnosti, sprečavanju i ublažavanju rizika te osigurati da svi relevantni dionici djeluju na temelju zajedničkog skupa pravila.

***Mjera 13.**: Komisija će objaviti smjernice vlasnicima pametnih mreža kako bi ojačali kibernetičku sigurnost svojih instalacija. U kontekstu inicijative za dizajn tržišta električne energije Komisija će razmotriti predlaganje planova za pripravnost na rizik i postupovnih pravila za razmjenu informacija i osiguravanje solidarnosti među državama članicama u vrijeme krize, uključujući pravila o prevenciji i ublažavanju kibernetičkih napada.*

4.4.3. Osiguravanje stabilnih financijskih sustava

Za funkcioniranje gospodarstva EU-a potreban je siguran financijski i platni sustav. Ključna je zaštita financijskog sustava i njegove infrastrukture od kibernetičkih napada, neovisno o motivu ili prirodi napadača. Za suzbijanje hibridnih prijetnji financijskim uslugama EU-a potrebno je da industrija razumije prijetnju, da je testirala svoju obranu te da ima potrebnu tehnologiju za zaštitu industrije od napada. Stoga je ključna razmjena informacija među sudionicima financijskih tržišta i s odgovarajućim nadležnim tijelima te ključnim pružateljima usluga ili korisnicima tih usluga, ali ta razmjena isto tako treba biti sigurna te ispunjavati zahtjeve zaštite podataka. U skladu s radom u međunarodnim forumima, uključujući rad skupine G7 u ovom sektoru, Komisija će nastojati utvrditi čimbenike koji ometaju odgovarajuću razmjenu informacija o prijetnjama te će predložiti rješenja. Važno je osigurati redovito testiranje i daljinu razradu protokola radi zaštite poslovne i odgovarajuće infrastrukture, uključujući neprekidnu nadogradnju tehnologije za jačanje sigurnosti.

***Mjera 14.**: Komisija će u suradnji s ENISA-om[41], državama članicama te relevantnim međunarodnim, europskim i nacionalnim nadležnim tijelima i financijskim institucijama promicati i unaprjeđivati platforme i mreže za razmjenu informacija o prijetnjama te rješavati čimbenike koji ometaju razmjenu takvih informacija.*

4.4.4. Promet

Moderni prometni sustavi (željeznički, cestovni, zračni, pomorski) oslanjaju se na informacijske sustave koji su osjetljivi na kibernetičke napade. S obzirom na prekograničnu dimenziju, EU u tom području ima posebnu ulogu. Komisija će u suradnji

[39] Centar EU-a za razmjenu informacija o incidentima i prijetnjama – ITIS.
[40] U obliku Platforme stručnjaka za energetiku u području kibernetičke sigurnosti (EECSP).
[41] Agencija Europske unije za mrežnu i informacijsku sigurnost

s državama članicama i dalje analizirati kibernetičke prijetnje i rizike povezane s nezakonitim uplitanjem u prometne sustave. Komisija razvija plan o kibernetičkoj sigurnosti zračnog prometa u suradnji s Europskom agencijom za sigurnost zračnog prometa (EASA).[42] Kibernetičke prijetnje sigurnosnoj zaštiti u pomorstvu nastoje se otkloniti i u okviru Strategije Europske unije za sigurnosnu zaštitu u pomorstvu i njezinog Akcijskog plana.

<u>Mjera 15.</u>: Komisija i Visoka predstavnica će (u okviru svojih područja nadležnosti) u suradnji s državama članicama ispitati način postupanja u slučaju hibridne prijetnje, posebno one koja se odnosi na kibernetičke napade diljem prometnog sektora.

4.5. Usmjeravanje na financiranje hibridnih prijetnji

Počiniteljima hibridnih prijetnji potrebno je financiranje kako bi nastavili svoje aktivnosti. Financiranje se može upotrijebiti za potporu terorističkim skupinama ili suptilnije oblike destabilizacije, kao što je financiranje interesnih skupina i rubnih političkih stranaka. EU je pojačao napore u borbi protiv financiranja kriminala i terorizma, kao što je navedeno u Europskom programu sigurnosti, posebno u Akcijskom planu.[43] U tom se kontekstu revidiranim europskim okvirom za suzbijanje pranja novca pojačava borba protiv financiranja terorizma i pranja novca te olakšava rad nacionalnih financijsko-obavještajnih jedinica (FIU) kako bi se utvrdile i pratile sumnjive novčane transakcije i razmjene informacija, istodobno osiguravajući sljedivost prijenosa sredstava u Europskoj uniji. Stoga bi se njime isto tako moglo doprinijeti suzbijanju hibridnih prijetnji. U kontekstu instrumenata ZVSP-a mogu se istražiti prilagođene i učinkovite mjere ograničavanja za suzbijanje hibridnih prijetnji.

<u>Mjera 16.</u>: Komisija će se koristiti provedbom Akcijskog plana za jačanje borbe protiv financiranja terorizma te i na taj način doprinijeti suzbijanju hibridnih prijetnji.

4.6. Jačanje otpornosti na radikalizaciju i nasilni ekstremizam

Iako teroristička djela i nasilni ekstremizam nisu sami po sebi hibridne prirode, počinitelji hibridnih prijetnji mogu se usmjeriti na ranjive članove društva i pridobiti ih, radikalizirajući ih s pomoću propagande i suvremenih komunikacijskih kanala (uključujući internetske društvene medije i zamjenske skupine).

U cilju uklanjanja ekstremističkog sadržaja na internetu, Komisija u kontekstu Strategije jedinstvenog digitalnog tržišta analizira potrebu za potencijalnim novim mjerama, uzimajući u obzir njihov utjecaj na temeljno pravo na slobodu izražavanja i informiranja.

[42] O novoj uredbi o EASA-i trenutno raspravljaju Europski parlament i Vijeće nastavno na prijedlog Komisije iz prosinca 2015. Prijedlog uredbe Europskog parlamenta i Vijeća o zajedničkim pravilima u području civilnog zrakoplovstva i osnivanju Agencije Europske unije za sigurnost zračnog prometa te stavljanju izvan snage Uredbe (EZ) br. 216/2008 Europskog parlamenta i Vijeća – COM(2015) 613 final, 2015/0277 (COD)

[43] Komunikacija Komisije Europskom parlamentu i Vijeću o Akcijskom planu za jačanje borbe protiv financiranja terorizma – (COM(2016) 50 final)

To bi moglo uključivati stroge postupke za uklanjanje nezakonitog sadržaja izbjegavajući uklanjanje legalnog sadržaja („obavještavanje i djelovanje") te veću odgovornost i dubinsku analizu koju će provoditi posrednici u upravljanju svojim mrežama i sustavima. Time bi se trebao nadopuniti postojeći pristup na dobrovoljnoj osnovi, u kojem internet i poduzeća društvenih mreža (posebno u okviru internetskog foruma EU-a) u suradnji s jedinicom EU-a pri Europolu za rad u vezi s prijavljenim internetskim sadržajima brzo uklanjaju terorističku propagandu.

U kontekstu Europskog programa sigurnosti radikalizacija se suzbija razmjenom iskustava i razvojem najboljih praksi, uključujući suradnju u trećim zemljama. Cilj je Savjetodavne skupine za strateško komuniciranje u vezi sa Sirijom ponovno ojačati razvoj i širenje alternativnih poruka za suzbijanje terorističke propagande. Mreža za osvješćivanje o radikalizaciji podupire države članice i stručnjake koji trebaju surađivati s radikaliziranim pojedincima (uključujući strane terorističke borce) ili s osobama koje se smatraju podložnima radikalizaciji. Mreža za osvješćivanje o radikalizaciji organizira osposobljavanja i daje savjete te će pružiti potporu prioritetnim trećim zemljama koje su spremne na suradnju. Nadalje, Komisija potiče pravosudnu suradnju među dionicima u okviru kaznenopravnog sustava, uključujući Eurojust, kako bi se suzbili terorizam i radikalizacija diljem država članica, među ostalim i postupanje sa stranim terorističkim borcima i povratnicima.

Dopunjujući spomenute pristupe u okviru svojih **vanjskih djelovanja**, EU doprinosi suzbijanju nasilnog ekstremizma, među ostalim vanjskim angažmanom i informiranjem, prevencijom (suzbijanjem radikalizacije i financiranja terorizma), kao i s pomoću mjera za rješavanje temeljnih gospodarskih, političkih i društvenih čimbenika kojima se omogućava razvoj terorističkih skupina.

<u>Mjera 17.:</u> Komisija provodi mjere protiv radikalizacije koje su utvrđene u Europskom programu sigurnosti i analizira potrebu za ponovnim jačanjem postupaka uklanjanja nezakonitog sadržaja, pozivajući posrednike da provedu dubinsku analizu u upravljanju mrežama i sustavima.

4.7. Jačanje suradnje s trećim zemljama

Kao što je navedeno u Europskom programu sigurnosti, veći je naglasak EU-a na jačanju kapaciteta sektora sigurnosti u ***partnerskim zemljama***, među ostalim jačanjem poveznica između sigurnosti i razvoja te razvojem sigurnosne dimenzije revidirane Europske politike susjedstva.[44] Tim se mjerama isto tako može poticati otpornost partnera na hibridne aktivnosti.

Komisija namjerava dodatno pojačati razmjenu operativnih i strateških informacija sa zemljama kandidatkinjama te, ako je potrebno, unutar Istočnog partnerstva i južnog susjedstva u borbi protiv organiziranog kriminala, terorizma, nezakonite migracije i

[44] Zajednička komunikacija Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija – Preispitivanje Europske politike susjedstva, 18.11.2015., JOIN(2015) 50 final

trgovine malim oružjem. U borbi protiv terorizma EU pojačava suradnju s trećim zemljama uspostavljanjem poboljšanih sigurnosnih dijaloga i akcijskih planova.

Cilj je instrumenata EU-a za vanjsko financiranje stvaranje funkcionalnih i odgovornih institucija u trećim zemljama[45] koje su preduvjet za djelotvoran odgovor na sigurnosne prijetnje i jačanje otpornosti. U tom su kontekstu ključni alati reforma sigurnosnog sektora i izgradnja kapaciteta za potporu sigurnosti i razvoju.[46] U okviru Instrumenta za doprinos stabilnosti i miru[47] Komisija je razvila mjere za jačanje kibernetičke otpornosti i sposobnosti partnera za otkrivanje kibernetičkih napada i kriminala te odgovor na njih, a s pomoću tih mjera moguće je suzbiti hibridne prijetnje u trećim zemljama. EU financira aktivnosti izgradnje kapaciteta u partnerskim zemljama kako bi se ublažili sigurnosni rizici u vezi s KBRN pitanjima.[48]

Konačno, države članice bi u duhu sveobuhvatnog pristupa upravljanju krizom mogle primijeniti alate i misije zajedničke sigurnosne i obrambene politike (ZSOP), neovisno ili pridonoseći donesenim instrumentima EU-a kako bi pomogle partnerima da ojačaju vlastite kapacitete. Mogle bi se uzeti u obzir sljedeće mjere: i. potpora strateškoj komunikaciji, ii. savjetodavna potpora ključnim ministarstvima izloženima hibridnim prijetnjama; iii. dodatna potpora upravljanju granicama u hitnim slučajevima. Mogle bi se istražiti daljnje sinergije među instrumentima ZSOP-a i sigurnosnih, carinskih i pravnih dionika, uključujući relevantne agencije EU-a,[49] INTERPOL i Europske žandarmerijske snage, u skladu s njihovim nadležnostima.

<u>Mjera 18.</u>: Visoka predstavnica će u suradnji s Komisijom pokrenuti pregled rizika hibridnih prijetnji u susjednim regijama.

Visoka predstavnica, Komisija i države članice koristit će se instrumentima koji su im na raspolaganju kako bi izgradili kapacitete partnera i ojačali njihovu otpornost na hibridne prijetnje. Misije ZSOP-a mogle bi se koristiti za pomoć partnerima u jačanju njihovih kapaciteta, neovisno ili pridonoseći instrumentima EU-a.

5. SPREČAVANJE KRIZE, ODGOVOR NA KRIZU I OPORAVAK

Kao što je navedeno u odjeljku 3.1., predložena jedinica EU-a za otkrivanje hibridnih prijetnji nastoji analizirati relevantne pokazatelje kako bi se moglo odgovoriti na hibridne

[45] Isto; Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija, Strategija proširenja EU-a, 10.11.2015., COM(2015) 611 final; Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija, Povećanje učinka razvojne politike EU-a; Plan za promjenu, 13.10.2011., COM(2011) 637 final

[46] Zajednička komunikacija – Izgradnja kapaciteta kao potpora sigurnosti i razvoju – osposobljavanje partnera u sprečavanju kriza i upravljanju njima (JOIN(2015)17 final)

[47] Uredba (EU) br. 230/2014 Europskog parlamenta i Vijeća od 11. ožujka 2014. o uspostavi Instrumenta za doprinos stabilnosti i miru, SL L 77, 15.3.2014.

[48] Obuhvaćena područja uključuju nadzor granica, upravljanje krizom, prvi odgovor, borbu protiv krijumčarenja, kontrolu izvoza robe s dvojnom namjenom, nadzor i kontrolu bolesti, nuklearnu forenziku, oporavak nakon incidenta i zaštitu visokorizičnih objekata. Najbolje prakse razvijene u okviru Akcijskog plana EU-a u području KBRN-a, kao što su Europski centar za obuku u području nuklearne sigurnosti i sudjelovanje EU-a u Međunarodnoj radnoj skupini za praćenje granice, mogu se razmijeniti s trećim zemljama.

[49] EUROPOL, FRONTEX, CEPOL, EUROJUST

prijetnje, spriječiti ih te obavijestiti donositelje odluka u EU-u. Iako se dugoročnim politikama na nacionalnoj razini i razini EU-a može smanjiti izloženost, u kratkom je roku i dalje ključno ojačati sposobnost država članica i Unije za sprečavanje, odgovor na hibridne prijetnje i oporavak od hibridnih prijetnji na brz i koordiniran način.

Ključan je brz odgovor na događaje koje su uzrokovale hibridne prijetnje. U tom pogledu, olakšavanje mjera i kapaciteta nacionalne civilne zaštite koje provodi Europski koordinacijski centar za odgovor na hitne situacije[50] mogao bi biti učinkovit mehanizam brzog odgovora za aspekte hibridnih prijetnji koji zahtijevaju odgovor civilne zaštite. To bi se moglo postići u suradnji s drugim EU-ovim mehanizmima odgovora i sustavima ranog upozorenja, posebno sa Situacijskom sobom ESVD-a u području vanjskih sigurnosnih dimenzija i s Centrom za stratešku analizu i odgovor u području unutarnje sigurnosti.

Klauzulom solidarnosti (članak 222. UFEU-a) omogućuje se djelovanje Unije i djelovanje među državama članicama ako je država članica meta terorističkog napada ili žrtva prirodne katastrofe ili katastrofe uzrokovane ljudskim djelovanjem. Djelovanje Unije u korist države članice osigurano je primjenom Odluke Vijeća 2014/415/EU.[51] Dogovori za koordinaciju unutar Vijeća trebali bi se oslanjati na EU-ov integrirani odgovor na političku krizu.[52] U okviru tih dogovora Komisija i Visoka predstavnica će (u okviru svojih područja nadležnosti) utvrditi relevantne instrumente Unije i podnijeti prijedloge Vijeću za odluke o izvanrednim mjerama.

Članak 222. UFEU-a obuhvaća i situacije koje se odnose na izravnu pomoć jedne države članice ili više njih državi članici koja je bila žrtva terorističkog napada ili katastrofe. U tom se pogledu odluka Vijeća 2014/415/EU ne primjenjuje. S obzirom na nejasnoće povezane s hibridnim aktivnostima, Komisija i Visoka predstavnica (u okviru svojih područja nadležnosti) ocijenit će posljednju moguću primjenu klauzule solidarnosti ako je država članica izložena znatnim hibridnim prijetnjama.

Za razliku od članka 222. UFEU-a, moguće je pozivanje na članak 42. stavak 7. UEU-a kako bi se pružio prikladan i pravodoban odgovor ako višestruke ozbiljne hibridne prijetnje predstavljaju oružanu agresiju protiv države članice EU-a. Sveobuhvatna i ozbiljna manifestacija hibridnih prijetnji može zahtijevati povećanu suradnju i koordinaciju s NATO-om.

Države članice potiču se da uzmu u obzir potencijalne hibridne prijetnje pri pripremanju svojih snaga. Kako bi bile pripremljene donositi odluke brzo i učinkovito u slučaju hibridnog napada, države članice trebaju redovito održavati vježbe na radnoj i političkoj razini kako bi ispitale sposobnost donošenja odluka u nacionalnim i međunarodnim područjima. Cilj je uspostava zajedničkog operativnog protokola među državama članicama, Komisijom i Visokom predstavnicom navodeći učinkovite postupke u slučaju

[50] http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en
[51] Odluka Vijeća 2014/415/EU o aranžmanima Unije za provedbu klauzule solidarnosti, OJ L 192, 1.7.2014., str. 53.
[52] http://www.consilium.europa.eu/hr/documents-publications/publications/2014/eu-ipcr/

hibridnih prijetnji, od početne faze identifikacije do posljednje faze napada te utvrđujući ulogu svake institucije Unije i svakog dionika u procesu.

Kao važan dio ZSOP-a, dogovorom bi moglo biti omogućeno: (a) civilno i vojno osposobljavanje; (b) mentori i savjetodavne misije kojima bi se poboljšalo stanje sigurnosti i obrambene sposobnosti države kojoj se prijeti; (c) planiranje djelovanja u nepredvidivim situacijama kako bi se mogli utvrditi znakovi hibridnih prijetnji i ojačati sposobnosti ranog upozoravanja; (d) potpora upravljanju graničnim kontrolama u slučaju opasnosti; (e) potpora u specijaliziranim područjima, kao što su ublažavanje rizika KBRN-a i nevojne evakuacije.

***Mjera 19.**: Visoka predsjednica i Komisija će u suradnji s državama članicama uspostaviti zajednički operativni protokol i izvršiti redovite vježbe kako bi se poboljšala sposobnost donošenja strateških odluka kao odgovor na složene hibridne prijetnje na temelju postupaka u upravljanju krizom i integriranog političkog odgovora na krize.*

***Mjera 20.**: Komisija i visoka predstavnica će u okviru svojih područja nadležnosti ispitati primjenjivost i praktične posljedice primjene članka 222. UFEU-a i članka 42. stavka 7. UEU-a u slučaju dalekosežnog i ozbiljnog hibridnog napada.*

***Mjera 21.**: Visoka predstavnica će u suradnji s državama članicama uključiti, iskoristiti i koordinirati kapacitete vojnih akcija u suzbijanju hibridnih prijetnji u okviru zajedničke sigurnosne i obrambene politike.*

6. JAČANJE SURADNJE S NATO-OM

Hibridne prijetnje predstavljaju izazov za EU, ali i za druge velike partnerske organizacije, uključujući Ujedinjene narode (UN), Organizaciju za europsku sigurnost i suradnju (OESS) i posebno za NATO. Učinkovitim se odgovorom poziva na dijalog i koordinaciju među organizacijama na političkoj i operativnoj razini. Intenzivnijom bi se interakcijom EU-a i NATO-a obje organizacije mogle bolje pripremiti i učinkovitije odgovoriti na hibridne prijetnje na komplementaran način te uz uzajamnu potporu, na temelju načela uključivosti, istodobno poštujući autonomnost u donošenju odluka i pravila o zaštiti podataka svake organizacije.

Dvije organizacije dijele iste vrijednosti i suočavaju se sa sličnim izazovima. Države članice EU-a i saveznice NATO-a očekuju potporu od svojih organizacija te njihovu brzu, odlučnu i usklađenu reakciju u slučaju krize ili, u najboljem slučaju, sprečavanje krize. Utvrđen je niz područja u kojima je potrebna jača suradnja i koordinacija EU-a i NATO-a, uključujući uvid u stanje, strateške komunikacije, kibernetičku sigurnost te sprečavanje krize i odgovor na krizu. Aktualne neformalne dijaloge EU-a i NATO-a o hibridnim prijetnjama treba ojačati kako bi se mogle uskladiti aktivnosti dviju organizacija u tom području.

Kako bi se razvili odgovori EU-a/NATO-a koji se međusobno nadopunjuju, važno je da obje organizacije imaju isti uvid u stanje prije i tijekom krize. To se može postići redovitom razmjenom utvrđenih analiza i iskustava, ali i neposrednom vezom jedinice

EU-a za otkrivanje hibridnih prijetnji i njezinog pandana u NATO-u. Isto je tako važno izgraditi uzajamno razumijevanje međusobnih postupaka upravljanja krizom kako bi se osigurale brze i učinkovite reakcije. Otpornost bi se mogla ojačati osiguravanjem komplementarnosti u određivanju referentnih vrijednosti za ključne dijelove njihovih infrastruktura, kao i bliskom suradnjom u okviru strateške komunikacije i kibernetičke obrane. U potpunosti uključivim zajedničkim vježbama na političkoj i tehničkoj razini poboljšala bi se učinkovitost kapaciteta donošenja odluka dviju organizacija. Daljnjim istraživanjem mogućnosti osposobljavanja razvila bi se usporediva razina stručnosti u kritičnim područjima.

<u>Mjera 22.</u>: Visoka predstavnica u suradnji s Komisijom nastavit će neformalni dijalog i poticati koordinaciju i suradnju s NATO-om o uvidu u stanje, strateškim komunikacijama, kibernetičkoj sigurnosti i „prevenciji krize i odgovoru na krizu" radi suzbijanja hibridnih prijetnji, poštujući načela uključivosti i autonomije postupaka donošenja odluka svake organizacije.

7. ZAKLJUČCI

U ovoj se Zajedničkoj komunikaciji navode mjere kojima se nastoje suzbiti hibridne prijetnje i ojačati otpornost na razini EU-a i nacionalnoj razini, kao i otpornost partnera. Budući da je naglasak na **podizanju svijesti**, predloženo je donošenje namjenskih mehanizama za razmjenu informacija s državama članicama i koordinaciju kapaciteta EU-a radi omogućivanja strateških komunikacija. Naglašene su mjere kojima se **jača otpornost** u područjima poput kibernetičke sigurnosti, kritične infrastrukture, zaštite financijskih sustava od nezakonitog korištenja te nastojanja u suzbijanju nasilnog ekstremizma i radikalizacije. Za sva je ta područja prvi korak da EU i države članice provedu dogovorene strategije te da države članice u potpunosti provedu postojeće zakonodavstvo, a bit će iznijete i neke konkretnije mjere za jačanje tih nastojanja.

Kad je riječ o **sprečavanju, odgovoru na hibridne prijetnje i oporavku od hibridnih prijetnji**, predlaže se ispitati izvedivost primjene klauzule solidarnosti iz članka 222. UFEU-a (kao što je navedeno u relevantnoj Odluci) i članka 42. stavka 7. UEU-a u slučaju dalekosežnih i ozbiljnih hibridnih napada. Kapacitet donošenja strateških odluka može se ojačati uspostavljanjem zajedničkog operativnog protokola.

Konačno, predlaže se **jačanje suradnje** i **koordinacije među EU-om i NATO-om** u okviru zajedničkih nastojanja u suzbijanju hibridnih prijetnji.

U provedbi ovog zajedničkog okvira Visoka predstavnica i Komisija ustraju u pokretanju relevantnih instrumenata EU-a koji su im na raspolaganju. Važno je da EU zajedno s državama članicama radi na smanjivanju rizika povezanih s izlaganjem potencijalnim hibridnim prijetnjama državnih i nedržavnih dionika.